Государственное бюджетное профессиональное образовательное учреждение
«Южно-Уральский государственный колледж»

МЕТОДИЧЕСКАЯ РАЗРАБОТКА
Комбинированный урок

Выполнение проверки компьютера на наличие признаков заражения вредоносным программным обеспечением

Специальность: 09.02.07 Информационные системы и программирование

ОП.13 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Разработал преподаватель
Чераева О.А.

РАССМОТРЕНО:
На заседании ПЦК
«Информационных технологий»
от 25.09.23 протокол № 2
Председатель
ПЦК _____/Н.А.Назарова/

Челябинск, 2023

Методическая разработка учебного занятия

Учебная дисциплина: ОП.13 Информационная безопасность

Специальность: 09.02.07 Информационные системы ипрограммирование

Курс: 2

Тема занятия: Выполнение проверки компьютера на наличие признаков заражения вредоносным программным обеспечением

Вид занятия: комбинированное

Мотивация темы: обусловлена тем, что сегодня информация является ценным активом и необходимо осуществлять меры для ее защиты. Знания, навыки и умения, приобретенные в процессе изучения информационной безопасности, должны помочь студентам в процессе их дальнейшей профессиональной деятельности, а также в повседневной жизни.

Продолжительность занятия: 45 минут

Место проведения занятия: лекционная аудитория

Формирование профессиональной компетенции (ПК 9.8): обеспечивать защиту программного обеспечения компьютерных систем программными средствами

Цели занятия:

Обучающая*:*

- сформировать целостное представление об антивирусном программном обеспечении
- изучить основные компоненты антивирусного программного обеспечения на примере программы Kaspersky Endpoint Security;
- научить выполнять проверку компьютера на наличие заражения вредоносного программного обеспечения.

Развивающая:

- развивать память и логическое мышление;
- развивать речевую активность путем обогащения и усложнения словарного запаса;
- развивать коммуникативные навыки и навыки самоконтроля.

Воспитательная:

- вызвать интерес к изучению информационных технологий;
- возбудить готовность решать задачи самостоятельно.

По итогам обучения обучающийся должен:

Знать:

– виды антивирусных программ;

– принцип работы антивирусного программного обеспечения;

– признаки заражения компьютера вредоносным программным обеспечением.

Уметь:

– выполнять проверку компьютера антивирусным программным обеспечением.

Методы обучения, методические приемы: словесный; наглядный; практический.

Внутридисциплинарные связи: вредоносная программа, антивирусное программное обеспечение.

Междисциплинарные связи: ОП. 11 Компьютерные сети, ОП. 08 Основы проектирования баз данных, МДК.09.0 Обеспечение безопасности веб-приложений

Учебное оборудование (оснащение) занятия: ПК; мультимедийный проектор, антивирусное программное обеспечение Kaspersky Endpoint Security.

Методическое обеспечение занятия: опорный конспект, презентация; методические указания к практической работе.

Критерии и методы диагностики эффективности занятия: рефлексия, заполнение бланка.

Хронокарта занятия:

№ п/п	Этапы и содержание занятия	Время
1.	***Вступительная часть занятия***	**5 мин.**
1.1.	- Приветствие	
1.2.	- Тема занятия, мотивация темы	
1.3.	- Просмотр слайдов	
	- Оценка готовности аудитории и оборудования	
1.4.	- Цель занятия	
2.	***Актуализация опорных знаний***	**5 мин.**
2.1.	- Фронтальный опрос	
3.	***Выдача теоретического материала***	**15 мин.**
4.	***Закрепление изученного материала***	**10 мин.**
4.1.	- Выполнение задания на бланке	
5.	***Заключительная часть занятия***	**10 мин.**
5.1.	- Обобщение, рефлексия	
5.2.	- Выводы по теме	
5.4.	- Домашнее задание	

ХОД УРОКА

1. Вступительная часть занятия. Здравствуйте, ребята! Садитесь. Староста, сообщите, пожалуйста, кто отсутствует на занятии.

Сегодня мы с вами познакомимся с работой одной из антивирусных программ, научимся выполнять проверку компьютера на наличие вредоносного и нежелательного программного обеспечения (Презентация - Приложение 1).

Цель занятия: закрепить знания по теме «Признаки заражения компьютера вредоносным программным обеспечением; изучить основные компоненты антивирусного программного обеспечения на примере программы Kaspersky Endpoint Security.

2. Актуализация опорных знаний.

А для начала давайте вспомним, что мы проходили на прошлом занятии, и проверим, как вы подготовились к уроку. Желающий выйдет к доске нарисовать классификацию антивирусных программ,объяснить их особенности.

Фронтальный опрос:

1. Что называют вредоносной программой?
2. Какие виды вредоносного программного обеспечения вам известны?
3. По каким признакам можно узнать, что мобильное устройство заражено вредоносной программой?

Вредоносная программа – это универсальный термин для обозначения любого типа вредоносного программного обеспечения (сетевые черви, классические файловые вирусы, троянские программы, хакерские утилиты и пр.), предназначенного для нанесения вреда или эксплуатации программируемого устройства, службы или сети.

Виды вредоносного программного обеспечения:

- вирусы;
- черви;
- рекламное программное обеспечение;
- шпионское программное обеспечение;
- программы-вымогатели;
- боты;
- руткиты;
- троянские программы;

– баги.

При заражении компьютера могут появиться следующие признаки: резко снизившаяся скорость работы компьютера; непонятные и ранее не встречавшиеся ошибки в работе операционной системы; потребление большего количества Интернет-трафика; обнаружение файлов не в тех местах, где они были раньше; жалобы от знакомых на то, что им приходят от вас различные сообщения по e-mail непонятного характера; неожиданные сообщения от администрации онлайн-сервисов о том, что ваш аккаунт на сервисе заблокирован; прекращение работы антивирусной защиты или полное ее исчезновение; различные проблемы с установленным программным обеспечением; появление в автозагрузке операционной системы непонятных программ; не создаются папки/документы/ярлыки; странная работа клавиатуры, либо мыши; появление неожиданных папок и файлов; резкие сбои в работе USB-флеш-накопителя; самопроизвольное изменение прав пользователей; появление BSOD на компьютере; необъяснимые загрузки в безопасном режиме.

Проверка работы у доски

Различают следующие разновидности антивирусных программ: фильтры, или сторожа; детекторы; доктора, или фаги; ревизоры; иммунизаторы, или вакцины.

Фильтр представляет собой резидентную программу, которая контролирует опасные действия, характерные для вирусных программ, и запрашивает подтверждение на их выполнение.

Детекторы обеспечивают поиск и обнаружение вирусов в оперативной памяти и на внешних носителях.

Доктором называют антивирусную программу, позволяющую обнаруживать и обезвреживать вирусы.

Полифаг – программа, предназначенная для обнаружения и уничтожения компьютерных вирусов

Ревизор представляет собой программу, запоминающую исходное состояние программ, каталогов и системных областей и периодически сравнивающую текущее состояние с исходным.

Иммунизатор представляет собой резидентную программу, предназначенную для предотвращения заражения рядом известных вирусов путем их вакцинации.

3. Изложение нового материала.

Давайте подумаем:

- Для чего нужна антивирусное программное обеспечение?
- Какие антивирусные программы вы знаете?
- Какая антивирусная программа популярна в России?

Правильно Антивирус Касперского.

(Слайд 1)

1. Антивирусное программное обеспечение, разрабатываемое Лабораторией Касперского, относится к проприетарное программному обеспечению, т.е. является частной собственностью его правообладателей. На наших рабочих местах оно уже установлено, поэтому можем начать свою работу.
2. Для этого необходимо выполнить следующие действия:
3. Пуск —> Все программы —> Kaspersky Endpoint Security.

(Слайд 4)

После запуска программы нам открывается стартовое окно, которое показывает результаты защиты, технологии с помощью которых осуществляется защита системы и еще несколько функций, на которых мы остановимся чуть подробнее.

(Слайд 6)

Зайдем в «Компоненты защиты» здесь откроется две вкладки «Базовая защита» и «Продвинутая защита». Рассмотрим их по порядку.

Продвинутая защита состоит из следующих компонентов:

– Анализ поведения – это компонент, который обнаруживает угрозы на основе анализа поведения программ. Эффективен для обнаружения сложных угроз.

– Защита от эксплойтов – это компонент, который блокирует действия вредоносных программ, которые используют уязвимости в программном обеспечении.

– Предотвращение вторжений – это компонент, который регистрирует активность, совершаемую программами в системе, и регулирует деятельность программ в зависимости от их статуса.

– Откат вредоносных событий – это компонент, который собирает информацию о подозрительных действиях в системе не только в рамках текущей сессии работы, но и за время предыдущих сессий, что позволяет выполнить отмену всех совершенных

программой действий, если программа будет признана вредоносной.

Базовая защита состоит из следующих компонентов:

– Защита от файловых угроз – это компонент, который постоянно находится в оперативной памяти компьютера и проверяет все открытые, сохраняемые и запускаемые файлы.

– Защита от веб-угроз – компоненты, который защищает веб-трафик, поступающий на компьютер.

– Защита от сетевых угроз – компонент, который блокирует любую сетевую активность атакующего компьютера в отношении нашего компьютера.

Теперь вернемся назад и откроем вкладку «Компоненты защиты» —> Предотвращение вторжений

Здесь мы видим 3 вкладки: мониторинг активности программ, права программ, защищаемые ресурсы.

Мониторинг активности программ, показывает сводную информацию об активности и репутации программ, запущенных в текущий момент на компьютере.

Права программ определяют какие программы попадают в группу доверия.

Защищаемые ресурсы показывает какие ресурсы защищены от несанкционированного доступа к ним.

Нажмем «ОК» и выйдем из этой вкладки

(Слайд 8)

На стартовом окне откроем вкладку «Хранилище». В резервное хранилище помещают копии файлов, которые будут удалены или изменены в процессе лечения. Эти файлы хранятся в специальном формате и не представляют опасности.

Нажмем «ОК» и выйдем из этой вкладки

Итак, мы с Вами посмотрели из чего состоит антивирусное программное обеспечение Kaspersky Endpoint Security. Сейчас мы приступим к выполнению работы на компьютере.

4. Закрепление изученного материала

Запишите задание себе в тетрадь.

Открыть установленное антивирусное программное обеспечение на рабочем месте.

Проверить компьютер на наличие вирусного программного обеспечения

Открыть любую программу и найти ее в «Мониторинге активности программы» и посмотреть «репутацию» этой программы.

Если нет вопросов по выполнению задания, можете приступать, если возникнут вопросы по ходу выполнения, поднимайте руку, я к вам подойду.

Время выполнения практической работы 20-25 минут.

Все закончили? Давайте проверим!

Проверка работ осуществляется самими студентами (меняютсярядами).

Отлично, с практической работой все справились!

5. Проверка усвоения нового материала

А теперь вспомним, что нового мы узнали сегодня:

(Слайд 9)

- С какой антивирусной программой мы работали? *(Kaspersky Endpoint Security)?*
- Какие компоненты есть в базовой защите Kaspersky Endpoint Security? *(Защита от файловых угроз, защита от веб-угроз, защита от сетевых угроз)*

6. Подведение итогов занятия.

Вы славно потрудились. Практическую работу выполнили верно.

Новый материал усвоили. На следующий урок проверим насколько прочно.

Какие можно сделать выводы по теме?

Сообщение оценок.

7. Выдача домашнего задания. Проверить домашний персональный компьютер на наличие вредоносного программного обеспечения, с помощью установленного антивирусного программного обеспечения. При выполнении проверки описывать последовательность своих действий и делать скриншоты операций. По окончании работы сформировать отчет в программе MS Word.

8. Рефлексия

Преподаватель вместе со студентами подводят итоги урока, формируют рефлексивные навыки с помощью опорного алгоритмасамоанализа:

- на уроке я узнал...
- на уроке я понял...
- на уроке я научился...
- лучше всего на занятии у меня получалось...

- основные трудности были... Спасибо за урок. До свидания!

Методическое обеспечение занятия:

1. Нестеров, С. А. Основы информационной безопасности: учебник для СПО / С. А. Нестеров. — 2-е изд., стер. — Санкт-Петербург: Лань, 2022. — 324 с.

2. Партыка, Т. Л. Информационная безопасность: учеб. пособие / Т.Л. Партыка, И.И. Попов. — 5-е изд., перераб. и доп. — Москва: ФОРУМ: ИНФРА-М, 2021. — 432 с

3. Прохорова, О. В. Информационная безопасность и защита информации / О. В. Прохорова. — 4-е изд., стер. — Санкт-Петербург: Лань, 2023. — 124 с

4. Чераева О.А., Подин М.С. Информационная безопасность: электронное учебное пособие / О.А., Чераева, М.С. Подин. — Текст: электронный // Система электронного обучения ЮУГК. — URL: https://els.ecol.edu.ru/course/view.php?id=93 (дата обращения 30.09.2023). — Режим доступа: для авториз. Пользователей

5. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие / В.Ф. Шаньгин. — Москва: ФОРУМ: ИНФРА-М, 2021. — 416 с

Технологическая карта урока

ФИО педагогического работника: Чераева Ольга Александровна

Тип занятия: изучения и первичного закрепления новых знаний и способов деятельности

Дисциплина: ОП.13 Информационная безопасность

Тема: Выполнение проверки компьютера на наличие признаков заражения вредоносным программным обеспечением

Нормативные документы:

1) ФГОС СПО по специальности 09.02.07 Информационные системы и программирование

2) Учебная программа ОП.13 Информационная безопасность

С целью овладения профессиональными компетенциями обучающихся в ходе освоения дисциплины должен:

Уметь: выполнять проверку компьютера антивирусным программным обеспечением.

Знать:

- виды антивирусных программ
- принцип работы антивирусного программного обеспечения;
- признаки заражения компьютера вредоносным программным обеспечением;

Цель:

Обучающая: сформировать целостное представление об антивирусном программном обеспечении; изучить термины «вредоносное программное обеспечение», «антивирусное программное обеспечение», «вирус»; научиться выполнять проверку компьютера на наличие заражения вредоносного программного обеспечения.

Развивающая: развивать память и логическое мышление; развивать речевую активность путем обогащения и усложнения словарного запаса; развивать коммуникативные навыки и навыки самоконтроля.

Воспитательная: вызвать интерес к изучению информационных технологий; возбудить готовность решать задачи самостоятельно.

Форма занятия: комбинированный урок

Межпредметные связи: ОП. 11 Компьютерные сети, ОП. 08 Основы проектирования баз данных, МДК.09.0 Обеспечение безопасности веб-приложений

Структура занятия:

1. Сообщение темы и цели урока - 2 мин
2. Актуализация опорных знаний – 2 мин
3. Изложение нового материала - 15 мин
4. Закрепление изученного материала – 10 мин
5. Проверка усвоения нового материала - 5 мин
6. Подведение итогов занятия – 5 мин
7. Выдача домашнего задания - 1 мин
8. Рефлексия – 5 мин

Используемая литература:

1. Нестеров, С. А. Основы информационной безопасности: учебник для СПО / С. А. Нестеров. — 2-е изд., стер. — Санкт-Петербург: Лань, 2022. — 324 с.
2. Партыка, Т. Л. Информационная безопасность: учеб. пособие / Т.Л. Партыка, И.И. Попов. — 5-е изд., перераб. и доп. — Москва: ФОРУМ: ИНФРА-М, 2021. — 432 с
3. Прохорова, О. В. Информационная безопасность и защита информации / О. В. Прохорова. — 4-е изд., стер. — Санкт-Петербург: Лань, 2023. — 124 с
4. Чераева О.А., Подин М.С. Информационная безопасность: электронное учебное пособие / О.А., Чераева, М.С. Подин. — Текст: электронный // Система электронного обучения ЮУГК. — URL: https://els.ecol.edu.ru/course/view.php?id=93 (дата обращения 30.09.2023). — Режим доступа: для авториз. Пользователей
5. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие / В.Ф. Шаньгин. — Москва: ФОРУМ: ИНФРА-М, 2021. — 416 с

Ход урока

Этапы	Цель	Деятельность преподавателя	Деятельность студента	Результат
1. Сообщение темы и цели урока	Организация группы на урок Мотивация учебной деятельности	Приветствие обучающихся, проверка присутствующих	Приветствие преподавателя, подготовка к уроку	Готовность группы к уроку
Метод - словесный Методический приём-информационно-сообщающий Форма обучения - групповая Средства обучения - ПК, проектор				
2. Актуализация опорных знаний	Проверка знаний и умений обучающихся, актуализация знаний	Фронтальный опрос: вопросы по вредоносному программному обеспечению	Воспроизведение знаний при ответах на вопросы преподавателя	Готовность группы к восприятию новых знаний
Метод – словесный Методический приём - информационно-сообщающий Форма обучения – групповая Средства обучения - ПК, проектор				
3. Изложение нового материала	Обеспечение восприятия, первичного запоминания знаний и способов деятельности, связей и отношений в объекте изучения: изучение принципа работы антивирусной программы	Предъявление информации.	Восприятие и осознание знаний, их запоминание	Запись и первичное осмысление новых знаний.
Метод - Объяснительно-иллюстративный Методический приём- информационно-сообщающий Форма обучения - групповая Средства обучения – ПК, программа Kaspersky Endpoint Security				

4. Закрепление изученного материала	Обеспечение осмысления способов деятельности в объекте изучения: работа с компонентами антивирусной программы Kaspersky Endpoint Security	Организация действий учащихся с объектом изучения: программой Kaspersky Endpoint Security	Работа в Kaspersky Endpoint Security	Активные действия учащихся с объектом изучения: антивирусной программой Kaspersky Endpoint Security
Метод – репродуктивный Методический приём - выполнение задания с опорой на материал презентации Форма обучения - индивидуальная Средства обучения – ПК, программа Kaspersky Endpoint Security				
5. Проверка усвоения нового материала	Проверка усвоения новых знаний	Задает вопросы по изученной теме: с какой антивирусной программой мы работали? Какие компоненты есть в базовой защите Kaspersky Endpoint Security?	Отвечают на вопросы преподавателя	Адекватность самооценки обучающихся оценке преподавателя
Метод - словесный Методический прием – опрос по изученным функциям Форма контроля – фронтальная Средства обучения – ПК, программа Kaspersky Endpoint Security				
6. Подведение итогов занятия	Уточнение и разъяснение сложных моментов в новых знаниях	Поясняет особо трудные моменты лекции, выставление оценок	Задают вопросы преподавателю	Осмысление новых знаний
Метод - словесный Методический приём – информационно-сообщающий Форма обучения- фронтальная Средства обучения – ПК, программа Kaspersky Endpoint Security				
7. Выдача домашнего задания	Установление уровня осознанности выполнения домашнего задания	Озвучение требований к изучению пройденного материала	Осознание выполнения домашнего задания	Правильность выполнения домашнего задания

Метод - словесный Методический приём - запись на экране ПК Форма обучения - фронтальная Средства обучения - ПК, проектор				
8. Рефлексия	Мобилизация обучающихся на рефлексию своей деятельности	Выявляет сложности в освоении изученного материала.	Задают вопросы и отвечают на вопросы преподавателя	Открытость обучающихся в осмыслении своих действий и в их самооценке
Метод- словесный Методический приём - обобщение и выводы Форма обучения- фронтальная Средства обучения – ПК				